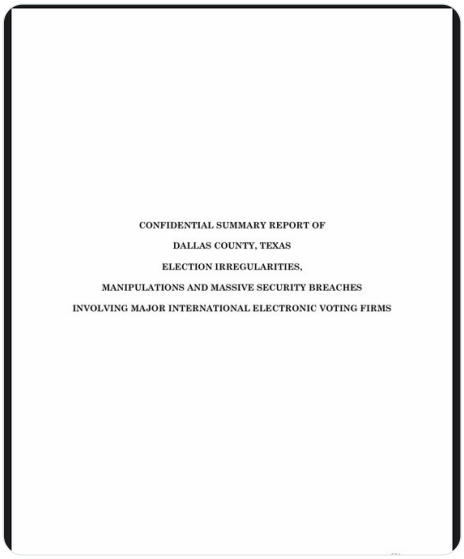
⚔️😽🌹 Bad Kitty 真相 🌹 😽⚔️ @pepesgrandma

7 Nov • 23 tweets • pepesgrandma/status/1325203412716154882

🚨🚨🚨 Breaking news folks! I have had some documents that were gifted to me from a journalist, and just got permission to burn everything down. Stay tuned!

The FBI refused to investigate previous electronic voter fraud for starts. And so much more!

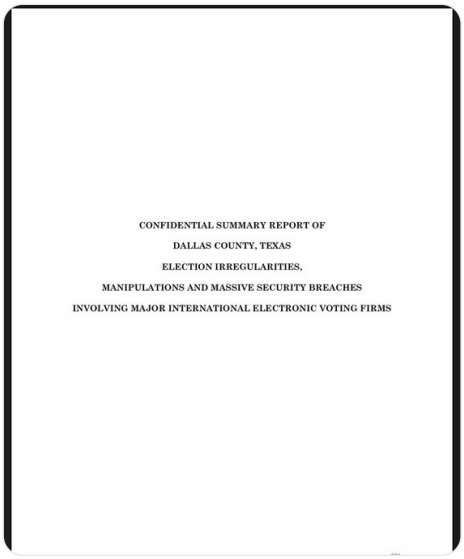
Thread: watch for updates


CONFIDENTIAL SUMMARY REPORT OF
DALLAS COUNTY, TEXAS
ELECTION IRREGULARITIES,
MANIPULATIONS AND MASSIVE SECURITY BREACHES
INVOLVING MAJOR INTERNATIONAL ELECTRONIC VOTING FIRMS


ELECTION FRAUD - A Real Threat to Our Democracy
Post Briefing Outline with all
Related Attachments (1 – 8)
Revised: August 28, 2020

Lets start with Dallas County Texas 2018. Pretty much what is happening right now, happened to them. And there are receipts. Coming up!

The FBI and Texas AG refused to do anything and Mitch McConnel didn't do anything either. Otherwise we would not be here today.



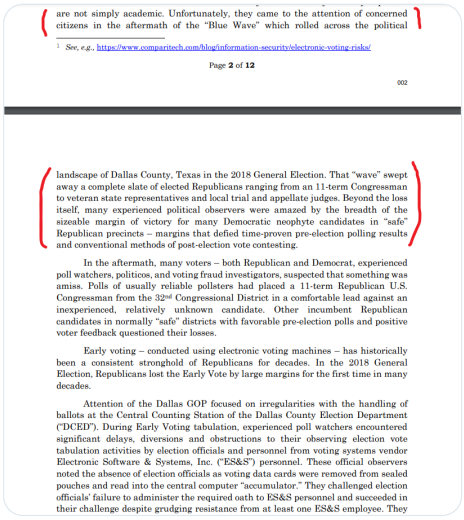
CONFIDENTIAL SUMMARY REPORT OF

DALLAS COUNTY, TEXAS

ELECTION IRREGULARITIES,

MANIPULATIONS AND MASSIVE SECURITY BREACHES

INVOLVING MAJOR INTERNATIONAL ELECTRONIC VOTING FIRMS



are not simply academic. Unfortunately, they came to the attention of concerned citizens in the aftermath of the "Blue Wave" which rolled across the political

[1] *See, e.g.*, https://www.comparitech.com/blog/information-security/electronic-voting-risks/

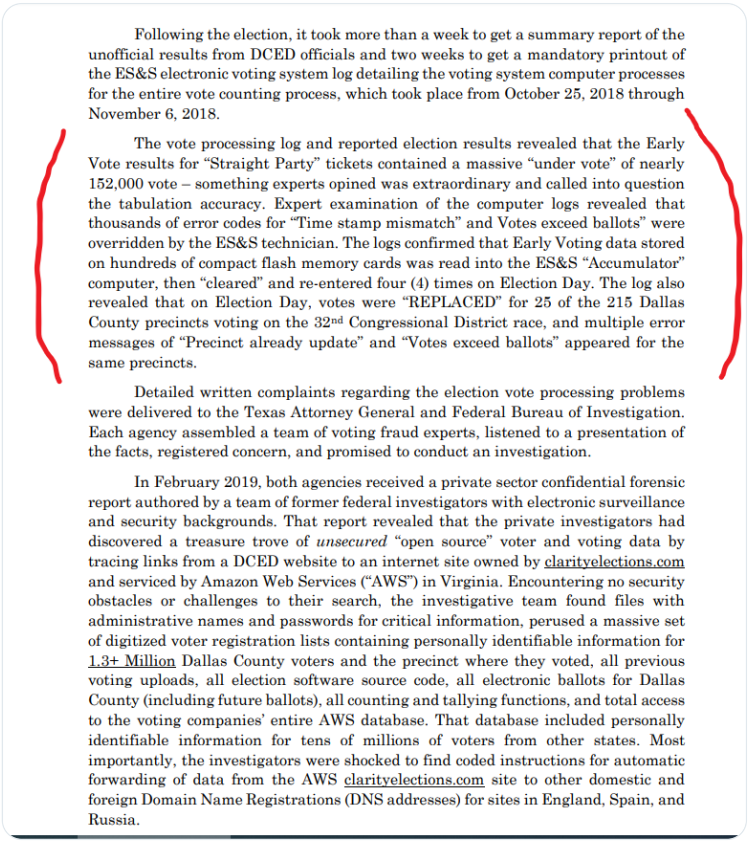
landscape of Dallas County, Texas in the 2018 General Election. That "wave" swept away a complete slate of elected Republicans ranging from an 11-term Congressman to veteran state representatives and local trial and appellate judges. Beyond the loss itself, many experienced political observers were amazed by the breadth of the sizeable margin of victory for many Democratic neophyte candidates in "safe" Republican precincts – margins that defied time-proven pre-election polling results and conventional methods of post-election vote contesting.

In the aftermath, many voters – both Republican and Democrat, experienced poll watchers, politicos, and voting fraud investigators, suspected that something was amiss. Polls of usually reliable pollsters had placed a 11-term Republican U.S. Congressman from the 32nd Congressional District in a comfortable lead against an inexperienced, relatively unknown candidate. Other incumbent Republican candidates in normally "safe" districts with favorable pre-election polls and positive voter feedback questioned their losses.

Early voting – conducted using electronic voting machines – has historically been a consistent stronghold of Republicans for decades. In the 2018 General Election, Republicans lost the Early Vote by large margins for the first time in many decades.

Attention of the Dallas GOP focused on irregularities with the handling of ballots at the Central Counting Station of the Dallas County Election Department ("DCED"). During Early Voting tabulation, experienced poll watchers encountered significant delays, diversions and obstructions to their observing election vote tabulation activities by election officials and personnel from voting systems vendor Electronic Software & Systems, Inc. ("ES&S") personnel. These official observers noted the absence of election officials as voting data cards were removed from sealed pouches and read into the central computer "accumulator." They challenged election officials' failure to administer the required oath to ES&S personnel and succeeded in their challenge despite grudging resistance from at least one ES&S employee. They

Expert examination of the computer logs revealed that thousands of error codes for "Time stamp mismatch" and Votes exceed ballots" were overridden by the ES&S technician. ETC.. Read the rest here ⬇️



Following the election, it took more than a week to get a summary report of the unofficial results from DCED officials and two weeks to get a mandatory printout of the ES&S electronic voting system log detailing the voting system computer processes for the entire vote counting process, which took place from October 25, 2018 through November 6, 2018.

The vote processing log and reported election results revealed that the Early Vote results for "Straight Party" tickets contained a massive "under vote" of nearly 152,000 vote – something experts opined was extraordinary and called into question the tabulation accuracy. Expert examination of the computer logs revealed that thousands of error codes for "Time stamp mismatch" and Votes exceed ballots" were overridden by the ES&S technician. The logs confirmed that Early Voting data stored on hundreds of compact flash memory cards was read into the ES&S "Accumulator" computer, then "cleared" and re-entered four (4) times on Election Day. The log also revealed that on Election Day, votes were "REPLACED" for 25 of the 215 Dallas County precincts voting on the 32nd Congressional District race, and multiple error messages of "Precinct already update" and "Votes exceed ballots" appeared for the same precincts.

Detailed written complaints regarding the election vote processing problems were delivered to the Texas Attorney General and Federal Bureau of Investigation. Each agency assembled a team of voting fraud experts, listened to a presentation of the facts, registered concern, and promised to conduct an investigation.

In February 2019, both agencies received a private sector confidential forensic report authored by a team of former federal investigators with electronic surveillance and security backgrounds. That report revealed that the private investigators had discovered a treasure trove of *unsecured* "open source" voter and voting data by tracing links from a DCED website to an internet site owned by clarityelections.com and serviced by Amazon Web Services ("AWS") in Virginia. Encountering no security obstacles or challenges to their search, the investigative team found files with administrative names and passwords for critical information, perused a massive set of digitized voter registration lists containing personally identifiable information for 1.3+ Million Dallas County voters and the precinct where they voted, all previous voting uploads, all election software source code, all electronic ballots for Dallas County (including future ballots), all counting and tallying functions, and total access to the voting companies' entire AWS database. That database included personally identifiable information for tens of millions of voters from other states. Most importantly, the investigators were shocked to find coded instructions for automatic forwarding of data from the AWS clarityelections.com site to other domestic and foreign Domain Name Registrations (DNS addresses) for sites in England, Spain, and Russia.

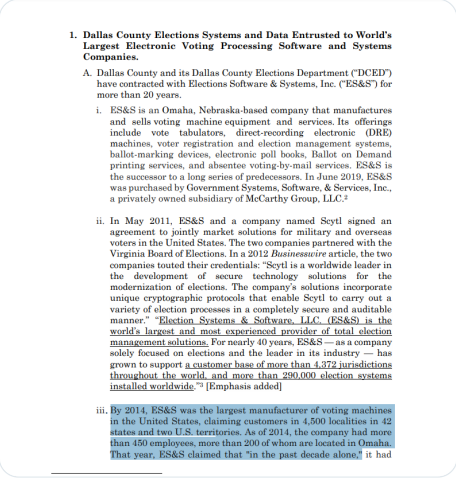
They destroyed the evidence before the 22 month retention date.

Notably, litigation contesting the bond election has revealed covert destruction of the ES&S equipment, software, and data storage devices used in the 2018 Primary and 2018 General Election in mid-July 2019.

Remarkably, the FBI and Texas Attorney General failed to interview identified witnesses, ignored the report, and quietly shelved their inquiries.

This report is the first of a series of reports regarding voting irregularities and DCED election officials' misconduct preceding and during elections. The authors are preparing additional reports concerning election issues with a May 2019 $1.1 Billion Dallas County Community College District bond election and the 2020 Super Tuesday primary. Notably, litigation contesting the bond election has revealed covert destruction of the ES&S equipment, software, and data storage devices used in the 2018 Primary and General Election in mid-July 2019. Texas law requires maintenance of all election records for federal elections for a period of 22 months.

By 2014, ES&S (Involved in Dallas County) was the largest manufacturer of voting machines in the US, claiming customers in 4,500 localities in 42 states and two U.S. territories. As of 2014, the company had more than 450 employees, more than 200 of whom are located in Omaha.



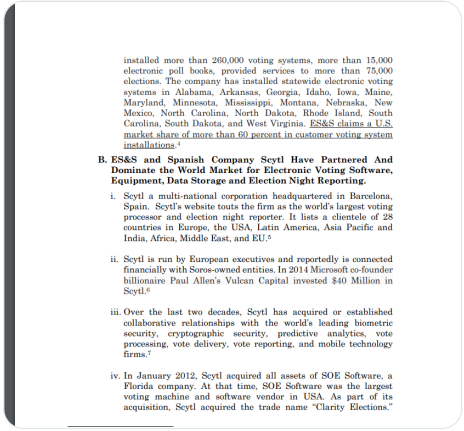
1. **Dallas County Elections Systems and Data Entrusted to World's Largest Electronic Voting Processing Software and Systems Companies.**

A. Dallas County and its Dallas County Elections Department ("DCED") have contracted with Elections Software & Systems, Inc. ("ES&S") for more than 20 years.

i. ES&S is an Omaha, Nebraska-based company that manufactures and sells voting machine equipment and services. Its offerings include vote tabulators, direct-recording electronic (DRE) machines, voter registration and election management systems, ballot-marking devices, electronic poll books, Ballot on Demand printing services, and absentee voting-by-mail services. ES&S is the successor to a long series of predecessors. In June 2019, ES&S was purchased by Government Systems, Software, & Services, Inc., a privately owned subsidiary of McCarthy Group, LLC.[3]

ii. In May 2011, ES&S and a company named Scytl signed an agreement to jointly market solutions for military and overseas voters in the United States. The two companies partnered with the Virginia Board of Elections. In a 2012 *Businesswire* article, the two companies touted their credentials: "Scytl is a worldwide leader in the development of secure technology solutions for the modernization of elections. The company's solutions incorporate unique cryptographic protocols that enable Scytl to carry out a variety of election processes in a completely secure and auditable manner." "Election Systems & Software, LLC. (ES&S) is the world's largest and most experienced provider of total election management solutions. For nearly 40 years, ES&S — as a company solely focused on elections and the leader in its industry — has grown to support a customer base of more than 4,372 jurisdictions throughout the world, and more than 290,000 election systems installed worldwide."[3] [Emphasis added]

iii. By 2014, ES&S was the largest manufacturer of voting machines in the United States, claiming customers in 4,500 localities in 42 states and two U.S. territories. As of 2014, the company had more than 450 employees, more than 200 of whom are located in Omaha. That year, ES&S claimed that "in the past decade alone," it had



installed more than 260,000 voting systems, more than 15,000 electronic poll books, provided services to more than 75,000 elections. The company has installed statewide electronic voting systems in Alabama, Arkansas, Georgia, Idaho, Iowa, Maine, Maryland, Minnesota, Mississippi, Montana, Nebraska, New Mexico, North Carolina, North Dakota, Rhode Island, South Carolina, South Dakota, and West Virginia. ES&S claims a U.S. market share of more than 60 percent in customer voting system installations.[4]

B. ES&S and Spanish Company Scytl Have Partnered And Dominate the World Market for Electronic Voting Software, Equipment, Data Storage and Election Night Reporting.

i. Scytl a multi-national corporation headquartered in Barcelona, Spain. Scytl's website touts the firm as the world's largest voting processor and election night reporter. It lists a clientele of 28 countries in Europe, the USA, Latin America, Asia Pacific and India, Africa, Middle East, and EU.[5]

ii. Scytl is run by European executives and reportedly is connected financially with Soros-owned entities. In 2014 Microsoft co-founder billionaire Paul Allen's Vulcan Capital invested $40 Million in Scytl.[6]

iii. Over the last two decades, Scytl has acquired or established collaborative relationships with the world's leading biometric security, cryptographic security, predictive analytics, vote processing, vote delivery, vote reporting, and mobile technology firms.[7]

iv. In January 2012, Scytl acquired all assets of SOE Software, a Florida company. At that time, SOE Software was the largest voting machine and software vendor in USA. As part of its acquisition, Scytl acquired the trade name "Clarity Elections."

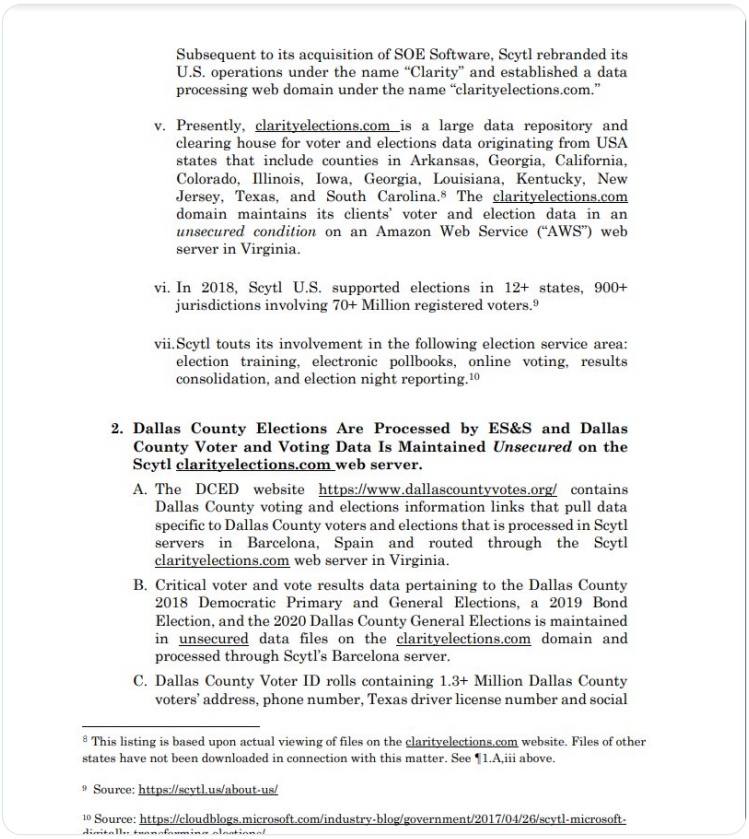
Critical voter and vote results data pertaining to elections, including the ➡️2020 General election ⬅️ is maintained in unsecured data files on the

Scytl Secure Election Technology

Scytl simplifies elections with secure election products. Scytl is a global leader in election technology solutions that simplify communication with your constituents, facilitate opportunities to inc…

http://clarityelections.com

domain and processed through Scytl's Barcelona server.



Subsequent to its acquisition of SOE Software, Scytl rebranded its U.S. operations under the name "Clarity" and established a data processing web domain under the name "clarityelections.com."

v. Presently, clarityelections.com is a large data repository and clearing house for voter and elections data originating from USA states that include counties in Arkansas, Georgia, California, Colorado, Illinois, Iowa, Georgia, Louisiana, Kentucky, New Jersey, Texas, and South Carolina.[8] The clarityelections.com domain maintains its clients' voter and election data in an *unsecured condition* on an Amazon Web Service ("AWS") web server in Virginia.

vi. In 2018, Scytl U.S. supported elections in 12+ states, 900+ jurisdictions involving 70+ Million registered voters.[9]

vii. Scytl touts its involvement in the following election service area: election training, electronic pollbooks, online voting, results consolidation, and election night reporting.[10]

2. Dallas County Elections Are Processed by ES&S and Dallas County Voter and Voting Data Is Maintained *Unsecured* on the Scytl clarityelections.com web server.

A. The DCED website https://www.dallascountyvotes.org/ contains Dallas County voting and elections information links that pull data specific to Dallas County voters and elections that is processed in Scytl servers in Barcelona, Spain and routed through the Scytl clarityelections.com web server in Virginia.

B. Critical voter and vote results data pertaining to the Dallas County 2018 Democratic Primary and General Elections, a 2019 Bond Election, and the 2020 Dallas County General Elections is maintained in unsecured data files on the clarityelections.com domain and processed through Scytl's Barcelona server.

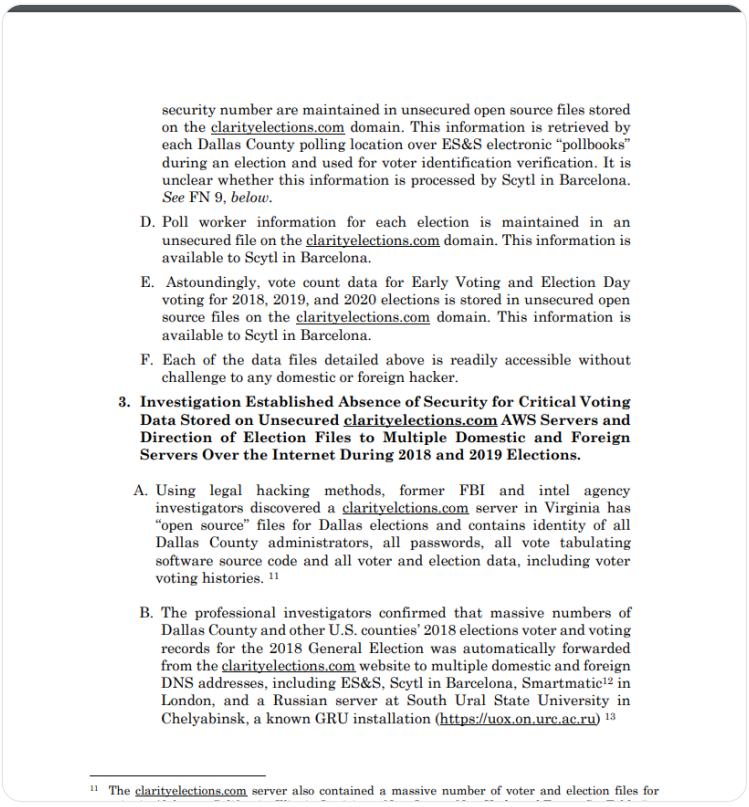
C. Dallas County Voter ID rolls containing 1.3+ Million Dallas County voters' address, phone number, Texas driver license number and social

[8] This listing is based upon actual viewing of files on the clarityelections.com website. Files of other states have not been downloaded in connection with this matter. See ¶1.A,iii above.

[9] Source: https://scytl.us/about-us/

[10] Source: https://cloudblogs.microsoft.com/industry-blog/government/2017/04/26/scytl-microsoft-

General Election voting records automatically forwarded from the Clarity website to multiple domestic and foreign DNS addresses, including ES&S, Scytl in Barcelona, Smartmatic12 in London, and Russian server at South Ural State University in Chelyabinsk, a known GRU installation



security number are maintained in unsecured open source files stored on the clarityelections.com domain. This information is retrieved by each Dallas County polling location over ES&S electronic "pollbooks" during an election and used for voter identification verification. It is unclear whether this information is processed by Scytl in Barcelona. *See* FN 9, *below*.

D. Poll worker information for each election is maintained in an unsecured file on the clarityelections.com domain. This information is available to Scytl in Barcelona.

E. Astoundingly, vote count data for Early Voting and Election Day voting for 2018, 2019, and 2020 elections is stored in unsecured open source files on the clarityelections.com domain. This information is available to Scytl in Barcelona.

F. Each of the data files detailed above is readily accessible without challenge to any domestic or foreign hacker.

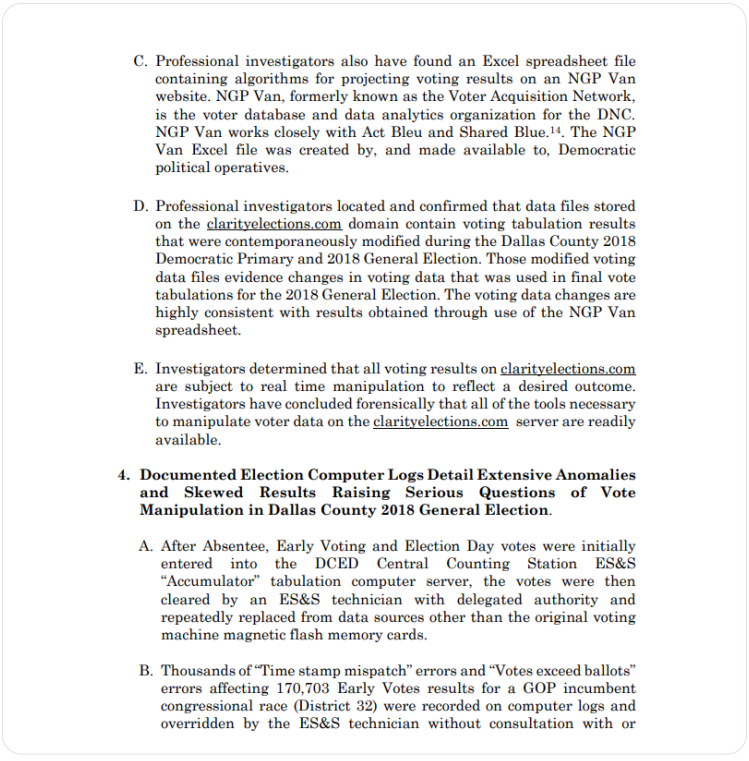
3. Investigation Established Absence of Security for Critical Voting Data Stored on Unsecured clarityelections.com AWS Servers and Direction of Election Files to Multiple Domestic and Foreign Servers Over the Internet During 2018 and 2019 Elections.

A. Using legal hacking methods, former FBI and intel agency investigators discovered a clarityelctions.com server in Virginia has "open source" files for Dallas elections and contains identity of all Dallas County administrators, all passwords, all vote tabulating software source code and all voter and election data, including voter voting histories. [11]

B. The professional investigators confirmed that massive numbers of Dallas County and other U.S. counties' 2018 elections voter and voting records for the 2018 General Election was automatically forwarded from the clarityelections.com website to multiple domestic and foreign DNS addresses, including ES&S, Scytl in Barcelona, Smartmatic[12] in London, and a Russian server at South Ural State University in Chelyabinsk, a known GRU installation (https://uox.on.urc.ac.ru) [13]

[11] The clarityelections.com server also contained a massive number of voter and election files for

Excel spreadsheet file containing algorithms for projecting voting results found on NGP Van website. NGP Van does voter database and analytics for DNC. NGP Van works closely with Act Bleu and Shared Blue. File was created by, and made available to, Democratic political operatives



C. Professional investigators also have found an Excel spreadsheet file containing algorithms for projecting voting results on an NGP Van website. NGP Van, formerly known as the Voter Acquisition Network, is the voter database and data analytics organization for the DNC. NGP Van works closely with Act Bleu and Shared Blue.[14]. The NGP Van Excel file was created by, and made available to, Democratic political operatives.

D. Professional investigators located and confirmed that data files stored on the clarityelections.com domain contain voting tabulation results that were contemporaneously modified during the Dallas County 2018 Democratic Primary and 2018 General Election. Those modified voting data files evidence changes in voting data that was used in final vote tabulations for the 2018 General Election. The voting data changes are highly consistent with results obtained through use of the NGP Van spreadsheet.

E. Investigators determined that all voting results on clarityelections.com are subject to real time manipulation to reflect a desired outcome. Investigators have concluded forensically that all of the tools necessary to manipulate voter data on the clarityelections.com server are readily available.

4. Documented Election Computer Logs Detail Extensive Anomalies and Skewed Results Raising Serious Questions of Vote Manipulation in Dallas County 2018 General Election.

A. After Absentee, Early Voting and Election Day votes were initially entered into the DCED Central Counting Station ES&S "Accumulator" tabulation computer server, the votes were then cleared by an ES&S technician with delegated authority and repeatedly replaced from data sources other than the original voting machine magnetic flash memory cards.

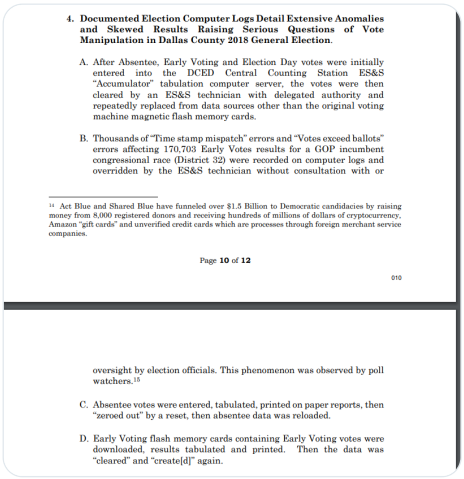
B. Thousands of "Time stamp mispatch" errors and "Votes exceed ballots" errors affecting 170,703 Early Votes results for a GOP incumbent congressional race (District 32) were recorded on computer logs and overridden by the ES&S technician without consultation with or

Documented Election Computer Logs Detail Extensive Anomalies and Skewed Results Raising Serious Questions of Vote Manipulation in Dallas County 2018

General Election.

Also, they obstructed Poll Watchers, and Engaged in Suspicious Conduct. Sound familiar?

Read here:



4. **Documented Election Computer Logs Detail Extensive Anomalies and Skewed Results Raising Serious Questions of Vote Manipulation in Dallas County 2018 General Election.**

A. After Absentee, Early Voting and Election Day votes were initially entered into the DCED Central Counting Station ES&S "Accumulator" tabulation computer server, the votes were then cleared by an ES&S technician with delegated authority and repeatedly replaced from data sources other than the original voting machine magnetic flash memory cards.

B. Thousands of "Time stamp mispatch" errors and "Votes exceed ballots" errors affecting 170,703 Early Votes results for a GOP incumbent congressional race (District 32) were recorded on computer logs and overridden by the ES&S technician without consultation with or

[14] Act Blue and Shared Blue have funneled over $1.5 Billion to Democratic candidacies by raising money from 8,000 registered donors and receiving hundreds of millions of dollars of cryptocurrency, Amazon "gift cards" and unverified credit cards which are processes through foreign merchant service companies.

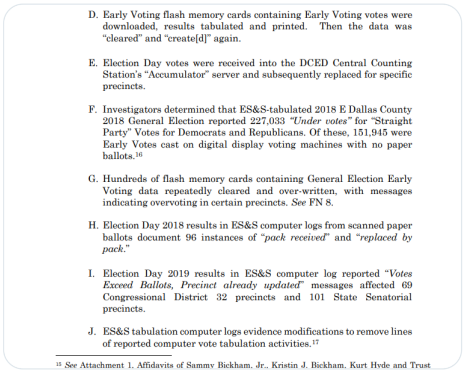
Page **10** of **12**

010

oversight by election officials. This phenomenon was observed by poll watchers.[15]

C. Absentee votes were entered, tabulated, printed on paper reports, then "zeroed out" by a reset, then absentee data was reloaded.

D. Early Voting flash memory cards containing Early Voting votes were downloaded, results tabulated and printed. Then the data was "cleared" and "create[d]" again.



D. Early Voting flash memory cards containing Early Voting votes were downloaded, results tabulated and printed. Then the data was "cleared" and "create[d]" again.

E. Election Day votes were received into the DCED Central Counting Station's "Accumulator" server and subsequently replaced for specific precincts.

F. Investigators determined that ES&S-tabulated 2018 E Dallas County 2018 General Election reported 227,033 *"Under votes"* for "Straight Party" Votes for Democrats and Republicans. Of these, 151,945 were Early Votes cast on digital display voting machines with no paper ballots.[16]

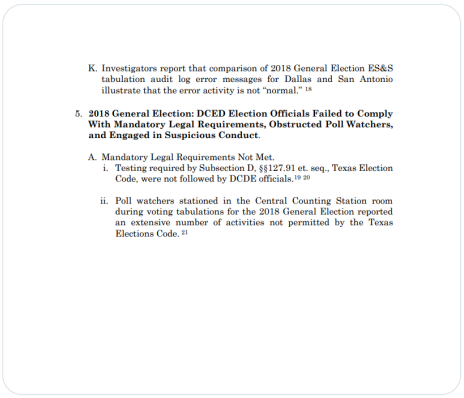
G. Hundreds of flash memory cards containing General Election Early Voting data repeatedly cleared and over-written, with messages indicating overvoting in certain precincts. *See* FN 8.

H. Election Day 2018 results in ES&S computer logs from scanned paper ballots document 96 instances of *"pack received"* and *"replaced by pack."*

I. Election Day 2019 results in ES&S computer log reported *"Votes Exceed Ballots, Precinct already updated"* messages affected 69 Congressional District 32 precincts and 101 State Senatorial precincts.

J. ES&S tabulation computer logs evidence modifications to remove lines of reported computer vote tabulation activities.[17]

[15] *See* Attachment 1, Affidavits of Sammy Bickham, Jr., Kristin J. Bickham, Kurt Hyde and Trust



K. Investigators report that comparison of 2018 General Election ES&S tabulation audit log error messages for Dallas and San Antonio illustrate that the error activity is not "normal." [18]

5. **2018 General Election: DCED Election Officials Failed to Comply With Mandatory Legal Requirements, Obstructed Poll Watchers, and Engaged in Suspicious Conduct.**

A. Mandatory Legal Requirements Not Met.

i. Testing required by Subsection D, §§127.91 et. seq., Texas Election Code, were not followed by DCDE officials.[19] [20]

ii. Poll watchers stationed in the Central Counting Station room during voting tabulations for the 2018 General Election reported an extensive number of activities not permitted by the Texas Elections Code. [21]

Ok this was the 12 page document, the 150 page one is up next. I need to make covfefe. Absorb this while I brew!

Nov 2019, we were asked to send a small team to Kentucky to look at the hugely anomalous gubernatorial race (SNIP- read below)

We had previously advised them that, based on our research, their race had all the earmarks of a potentially targeted race for vote tampering.

ELECTION FRAUD - A Real Threat to Our Democracy

Post Briefing Outline with all

Related Attachments (1 – 8)

Revised: August 28, 2020

Election Fraud – Narrative Briefing Outline – Shallow Dive – *Update August 28, 2020*

In 2017, Allied Special Operations Group, LLC ("ASOG") was formed as a security (cyber & personal investigations) support company for litigation, and various other commercial services as well as for limited, discreet government support. It is comprised of specialists in several areas including former operators from various 3 letter Federal agencies that have very deep cyber and HUMINT capabilities.

After the 2018 mid-term elections, we began an investigation into irregularities in election results using an 1,100-page Audit Log of the central tabulation server printed at the request of a citizen's group late on election night at the Dallas County Central Counting office. The audit logs included early vote totals as well as election night totals. The detailed logs documented entries into the tabulation system for the election itself and we saw many areas of concern.

In the audit logs of the Central Counting computer, we found vote totals in the database were zeroed out then reloaded several times between early vote ending and the Election Day close from sources outside of the election system. We also saw statistically strong evidence suggesting vote harvesting of under votes.

The ASOG cyber team in conjunction with other cyber experts took a deep dive into the election system and mapped the voting process from ballot casting to central tabulation to national collection and dissemination via SCYTL, a Spanish multinational corporation. Additionally, we mapped the top 5 or 6 of the major voting companies that are contracted by counties to run the bulk of our US elections (and around the world as well). Most Americans are unaware that our U.S. elections are run entirely by private companies under contract to counties, and these private companies and their independent retailers assemble the software, sell the machines, conduct the elections, keep the voter roles and information, collect the votes, tally the votes and post the results. All of this has virtually no transparency. Through Open Source Intel techniques and Tor contacts in the Dark Web, the experts could look into the source code of several of these companies and even see administrator level names and passwords for database access out in the open. They determined there were significant vulnerabilities in which unseen intruders could take advantage of, and actually change, votes. The investigation has lasted for 18 months.

In November 2019, we were asked to send a small team to Kentucky to look at the hugely anomalous gubernatorial race wherein every statewide race was won by Republicans with significant vote margins (200,000+ votes) except for the top of the ticket. The governor lost by 5,086 votes and members of his campaign thought something looked odd and wanted to get to the bottom of it. We had previously advised them that, based on our research, their race had all the earmarks of a potentially targeted race for vote tampering.

After the election, our cyber team uncovered a split second in the Kentucky election night video feed from Clarity Elections to CNN that actually displayed the findings of our investigation. (tbc) ⬇️

Within a few days after the election, our cyber team uncovered a split second in the election night video feed from Clarity Elections to CNN that actually displayed the findings of our investigation. This live feed from CNN accidentally showed reported votes to Governor Bevin ***decrease*** by 560 votes at the exact same instant his opponent, Andy Beshear, had an ***identical increase*** of 560 votes. This vote change is a 1,120 vote swing in a race that was decided by just over 5,000 votes hence about 20% of the vote swing is seen occurring in a split second with votes being subtracted from Bevin and added to Beshear. This can only demonstrate access into central tabulation, probably by uncredentialed outsiders changing vote totals virtually undetected and without an audit trail as we and others have demonstrated and written about. While several groups looked at the CNN clip, no one has been able to offer any other explanation of what we saw happen on CNN. CNN refused to comment. This video clip can be view on the EWR link Election Fraud Battle Plan.

In our briefing we show the clip and play it back to pause at the exact before and after frames where votes appear to have been switched. Additional clips have also been discovered.

We have begun to make public our election fraud information through various channels. We have recorded 4 explanatory video sessions, collected a compendium of many excellent source articles on this subject and supported several other investigatory groups.

We are now getting significant, national investigative reporters asking us to take them through our detailed 1-hour 15-minute briefing so they can choose the angle they want to write on. Starting Thursday, April 30th, articles started to appear on certain aspects of voter fraud and election fraud. See April 29, 2020 Western Journal: Cyber Experts Warning About 2020 Election.

Our decision to go public was based on the clock ticking towards the general election in November wherein altering the outcome of 3 or 4 key electoral states would change and defeat the actual will of the American people in selecting their President. Two other factors also determined this course. First, the President began to discuss requiring Voter ID in a COVID-19 Task Force Briefing that we took as a cue to move forward with disclosure, and secondly, on April 6, 2020, HBO launched (now on YouTube) an Election Fraud Documentary: "**Kill Chain**"

This was amazing timing. HBO released this 1 ½ hour documentary narrated by Hari Hursti the Finnish voter fraud cyber expert. In the documentary he shows how porous the system is, when 11, 12 and 15 year old kids are able to hack the election system in only minutes. He makes clear the ridiculous posture of various government officials who claim in hearings before Congress that the system is not connected to the internet and is not hackable. The much talked about "Certification" process is really only a voluntary guideline with no serious security elements. He puts into a documentary many of the things we have been saying for the last year.

This live feed from CNN accidentally showed reported votes to Gov Bevin (KY) decrease by 560 at the exact same instant his opponent, Andy Beshear, had an identical increase of 560 votes. This vote change is a 1,120 vote swing in a race decided >5,000 votes

https://www.youtube.com/embed/4h0pfQZcjjk

Not covered publicly -Is what we found out when we mapped the entire (Clarity Elections) network and its ownership and discovered a majority of the entire system rolls up to SCYTL, a Barcelona, Spain company.

What he did not cover is what we found out when we mapped the entire network and its ownership and discovered a majority of the entire system rolls up to SCYTL, a Barcelona, Spain company. It is SCYTL that has the final control on vote counting and reporting (and which the CNN video shows changing votes). Both the Chicago Sun Times and Forbes say it raises troubling concerns about election cyber security. Between SCYTL and another vote counting company, SGO Smartmatic, an amazing amount of the US Elections apparatus is held by, stored, and reported by foreign owned entities and often this data is held offshore. Worse yet, SCYTL declared bankruptcy in Barcelona, Spain on May 23rd of 2020 and at present it is not clear who the new owners actually are. But both companies incorporate extremely insecure and vulnerable systems for votes to be changed undetected. This seems like it should be a counter-intelligence issue.

Kill Chain **https://www.hbo.com/documentaries/kill-chain-the-cyber-war-on-americas**

Also see: The Election Fraud Battle Plan: A NEW LANDING PAGE on Kevin Freeman's Economic War Room was set up to aggregate articles and other resources. *(additional videos are added as needed)*

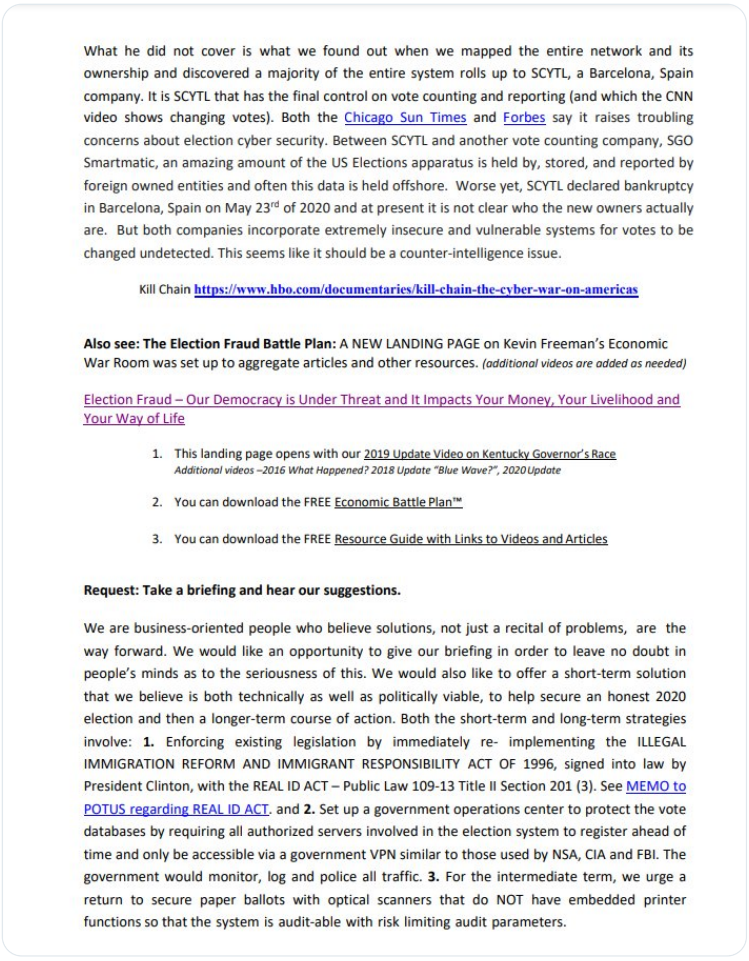
Election Fraud – Our Democracy is Under Threat and It Impacts Your Money, Your Livelihood and Your Way of Life

1. This landing page opens with our 2019 Update Video on Kentucky Governor's Race
   Additional videos –2016 What Happened? 2018 Update "Blue Wave?", 2020 Update
2. You can download the FREE Economic Battle Plan™
3. You can download the FREE Resource Guide with Links to Videos and Articles

Request: Take a briefing and hear our suggestions.

We are business-oriented people who believe solutions, not just a recital of problems, are the way forward. We would like an opportunity to give our briefing in order to leave no doubt in people's minds as to the seriousness of this. We would also like to offer a short-term solution that we believe is both technically as well as politically viable, to help secure an honest 2020 election and then a longer-term course of action. Both the short-term and long-term strategies involve: **1.** Enforcing existing legislation by immediately re- implementing the ILLEGAL IMMIGRATION REFORM AND IMMIGRANT RESPONSIBILITY ACT OF 1996, signed into law by President Clinton, with the REAL ID ACT – Public Law 109-13 Title II Section 201 (3). See MEMO to POTUS regarding REAL ID ACT. and **2.** Set up a government operations center to protect the vote databases by requiring all authorized servers involved in the election system to register ahead of time and only be accessible via a government VPN similar to those used by NSA, CIA and FBI. The government would monitor, log and police all traffic. **3.** For the intermediate term, we urge a return to secure paper ballots with optical scanners that do NOT have embedded printer functions so that the system is audit-able with risk limiting audit parameters.

It is SCYTL (Clarity Elections) that has the final control on vote counting and reporting (and which the CNN video shows changing votes). Both the Chicago Sun Times and Forbes say it raises troubling concerns about election cyber security.



What he did not cover is what we found out when we mapped the entire network and its ownership and discovered a majority of the entire system rolls up to SCYTL, a Barcelona, Spain company. It is SCYTL that has the final control on vote counting and reporting (and which the CNN video shows changing votes). Both the Chicago Sun Times and Forbes say it raises troubling concerns about election cyber security. Between SCYTL and another vote counting company, SGO Smartmatic, an amazing amount of the US Elections apparatus is held by, stored, and reported by foreign owned entities and often this data is held offshore. Worse yet, SCYTL declared bankruptcy in Barcelona, Spain on May 23rd of 2020 and at present it is not clear who the new owners actually are. But both companies incorporate extremely insecure and vulnerable systems for votes to be changed undetected. This seems like it should be a counter-intelligence issue.

Kill Chain **https://www.hbo.com/documentaries/kill-chain-the-cyber-war-on-americas**

Also see: The Election Fraud Battle Plan: A NEW LANDING PAGE on Kevin Freeman's Economic War Room was set up to aggregate articles and other resources. *(additional videos are added as needed)*

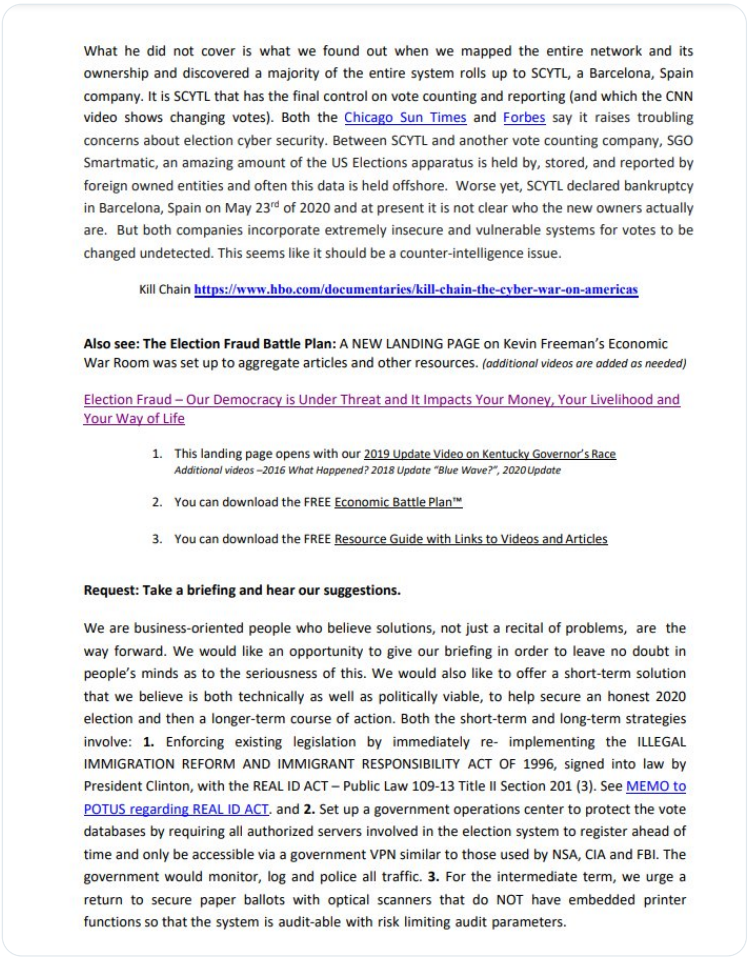
Election Fraud – Our Democracy is Under Threat and It Impacts Your Money, Your Livelihood and Your Way of Life

1. This landing page opens with our 2019 Update Video on Kentucky Governor's Race
   Additional videos –2016 What Happened? 2018 Update "Blue Wave?", 2020 Update
2. You can download the FREE Economic Battle Plan™
3. You can download the FREE Resource Guide with Links to Videos and Articles

Request: Take a briefing and hear our suggestions.

We are business-oriented people who believe solutions, not just a recital of problems, are the way forward. We would like an opportunity to give our briefing in order to leave no doubt in people's minds as to the seriousness of this. We would also like to offer a short-term solution that we believe is both technically as well as politically viable, to help secure an honest 2020 election and then a longer-term course of action. Both the short-term and long-term strategies involve: **1.** Enforcing existing legislation by immediately re- implementing the ILLEGAL IMMIGRATION REFORM AND IMMIGRANT RESPONSIBILITY ACT OF 1996, signed into law by President Clinton, with the REAL ID ACT – Public Law 109-13 Title II Section 201 (3). See MEMO to POTUS regarding REAL ID ACT. and **2.** Set up a government operations center to protect the vote databases by requiring all authorized servers involved in the election system to register ahead of time and only be accessible via a government VPN similar to those used by NSA, CIA and FBI. The government would monitor, log and police all traffic. **3.** For the intermediate term, we urge a return to secure paper ballots with optical scanners that do NOT have embedded printer functions so that the system is audit-able with risk limiting audit parameters.

Between SCYTL and another vote counting company, SGO
Smartmatic, an amazing amount of the US Elections apparatus is held by, stored, and reported by
foreign owned entities and often this data is held offshore.



What he did not cover is what we found out when we mapped the entire network and its ownership and discovered a majority of the entire system rolls up to SCYTL, a Barcelona, Spain company. It is SCYTL that has the final control on vote counting and reporting (and which the CNN video shows changing votes). Both the Chicago Sun Times and Forbes say it raises troubling concerns about election cyber security. Between SCYTL and another vote counting company, SGO Smartmatic, an amazing amount of the US Elections apparatus is held by, stored, and reported by foreign owned entities and often this data is held offshore. Worse yet, SCYTL declared bankruptcy in Barcelona, Spain on May 23rd of 2020 and at present it is not clear who the new owners actually are. But both companies incorporate extremely insecure and vulnerable systems for votes to be changed undetected. This seems like it should be a counter-intelligence issue.

Kill Chain **https://www.hbo.com/documentaries/kill-chain-the-cyber-war-on-americas**

Also see: The Election Fraud Battle Plan: A NEW LANDING PAGE on Kevin Freeman's Economic War Room was set up to aggregate articles and other resources. *(additional videos are added as needed)*

Election Fraud – Our Democracy is Under Threat and It Impacts Your Money, Your Livelihood and Your Way of Life

1. This landing page opens with our 2019 Update Video on Kentucky Governor's Race
   Additional videos –2016 What Happened? 2018 Update "Blue Wave?", 2020 Update
2. You can download the FREE Economic Battle Plan™
3. You can download the FREE Resource Guide with Links to Videos and Articles

Request: Take a briefing and hear our suggestions.

We are business-oriented people who believe solutions, not just a recital of problems, are the way forward. We would like an opportunity to give our briefing in order to leave no doubt in people's minds as to the seriousness of this. We would also like to offer a short-term solution that we believe is both technically as well as politically viable, to help secure an honest 2020 election and then a longer-term course of action. Both the short-term and long-term strategies involve: **1.** Enforcing existing legislation by immediately re- implementing the ILLEGAL IMMIGRATION REFORM AND IMMIGRANT RESPONSIBILITY ACT OF 1996, signed into law by President Clinton, with the REAL ID ACT – Public Law 109-13 Title II Section 201 (3). See MEMO to POTUS regarding REAL ID ACT. and **2.** Set up a government operations center to protect the vote databases by requiring all authorized servers involved in the election system to register ahead of time and only be accessible via a government VPN similar to those used by NSA, CIA and FBI. The government would monitor, log and police all traffic. **3.** For the intermediate term, we urge a return to secure paper ballots with optical scanners that do NOT have embedded printer functions so that the system is audit-able with risk limiting audit parameters.

"The foreign hosting of US voting information is therefore declared a national security concern and inconsistent with the letter and spirit of multiple U.S. laws including broad areas of Foreign Intelligence, the RICO Act, the Committee on Foreign Investment in the United States"

Possible Next Step for Cyber Security and the 2020 Election

COL (Ret) John R. Mills, Russell Ramsland and J. Keet Lewis

Action Item 3: Establishing the security of vote recording, aggregation of voting tallies, and cybersecurity of voter and voting results.

There is an assumption that vote recording, aggregation of voting tallies, and cybersecurity of voting results and related voting data are maintained in the United States with a transparent chain of custody visible and understandable to all election officials in the jurisdiction.

That is not the case and the complexity and lack of transparency combined with unclear chain of custody grievously undermines the process. Foreign hosting of live vote recording, voting tallies, and related voting information is actually quite common in the voting industry and often includes companies that are suspect in ownership and affiliation. In addition, there are often transfers of voting information through thumb drives and other portable media that are conducted without the competent oversight and assertation of election officials of all relevant political affiliations.

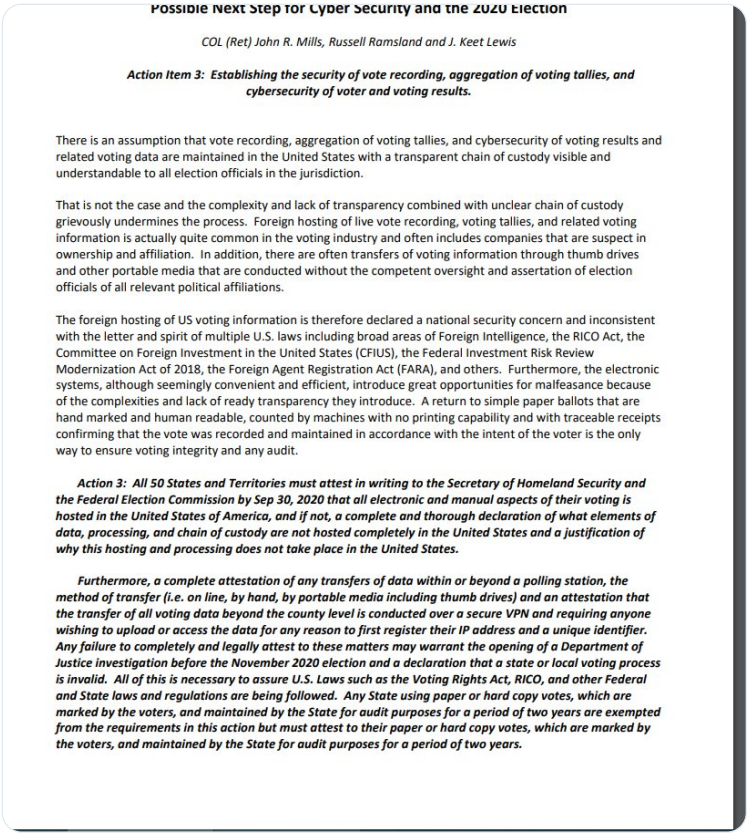
The foreign hosting of US voting information is therefore declared a national security concern and inconsistent with the letter and spirit of multiple U.S. laws including broad areas of Foreign Intelligence, the RICO Act, the Committee on Foreign Investment in the United States (CFIUS), the Federal Investment Risk Review Modernization Act of 2018, the Foreign Agent Registration Act (FARA), and others. Furthermore, the electronic systems, although seemingly convenient and efficient, introduce great opportunities for malfeasance because of the complexities and lack of ready transparency they introduce. A return to simple paper ballots that are hand marked and human readable, counted by machines with no printing capability and with traceable receipts confirming that the vote was recorded and maintained in accordance with the intent of the voter is the only way to ensure voting integrity and any audit.

Action 3: All 50 States and Territories must attest in writing to the Secretary of Homeland Security and the Federal Election Commission by Sep 30, 2020 that all electronic and manual aspects of their voting is hosted in the United States of America, and if not, a complete and thorough declaration of what elements of data, processing, and chain of custody are not hosted completely in the United States and a justification of why this hosting and processing does not take place in the United States.

Furthermore, a complete attestation of any transfers of data within or beyond a polling station, the method of transfer (i.e. on line, by hand, by portable media including thumb drives) and an attestation that the transfer of all voting data beyond the county level is conducted over a secure VPN and requiring anyone wishing to upload or access the data for any reason to first register their IP address and a unique identifier. Any failure to completely and legally attest to these matters may warrant the opening of a Department of Justice investigation before the November 2020 election and a declaration that a state or local voting process is invalid. All of this is necessary to assure U.S. Laws such as the Voting Rights Act, RICO, and other Federal and State laws and regulations are being followed. Any State using paper or hard copy votes, which are marked by the voters, and maintained by the State for audit purposes for a period of two years are exempted from the requirements in this action but must attest to their paper or hard copy votes, which are marked by the voters, and maintained by the State for audit purposes for a period of two years.

Action 3: All 50 States and Territories must attest in writing to the Secretary of Homeland Security and the Federal Election Commission by Sep 30, 2020 that all electronic and manual aspects of their voting is hosted in the United States of America,

So I'm certain they watched



Possible Next Step for Cyber Security and the 2020 Election

COL (Ret) John R. Mills, Russell Ramsland and J. Keet Lewis

Action Item 3: Establishing the security of vote recording, aggregation of voting tallies, and cybersecurity of voter and voting results.

There is an assumption that vote recording, aggregation of voting tallies, and cybersecurity of voting results and related voting data are maintained in the United States with a transparent chain of custody visible and understandable to all election officials in the jurisdiction.

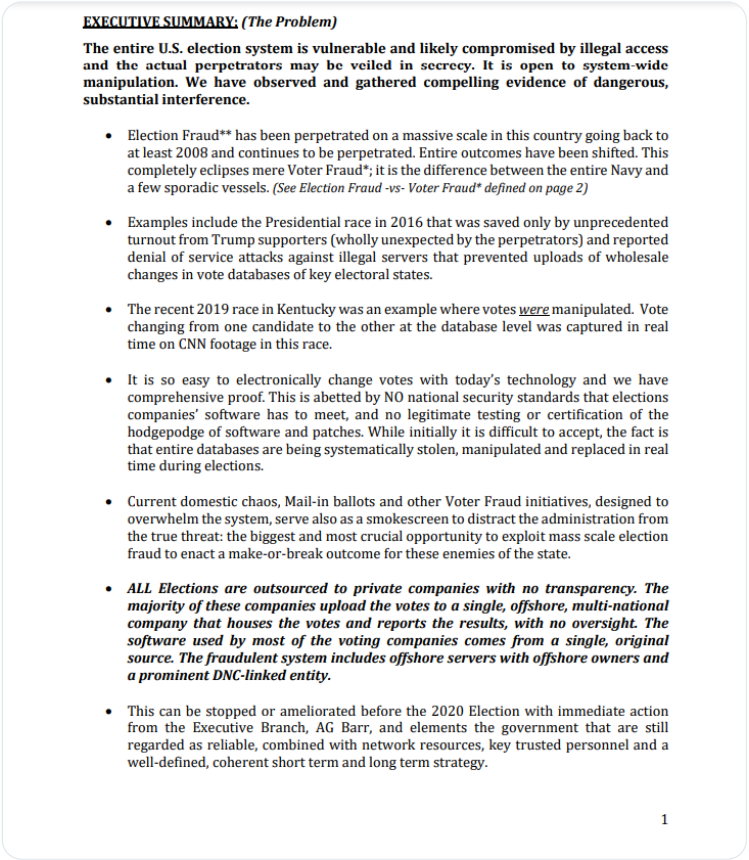
That is not the case and the complexity and lack of transparency combined with unclear chain of custody grievously undermines the process. Foreign hosting of live vote recording, voting tallies, and related voting information is actually quite common in the voting industry and often includes companies that are suspect in ownership and affiliation. In addition, there are often transfers of voting information through thumb drives and other portable media that are conducted without the competent oversight and assertation of election officials of all relevant political affiliations.

The foreign hosting of US voting information is therefore declared a national security concern and inconsistent with the letter and spirit of multiple U.S. laws including broad areas of Foreign Intelligence, the RICO Act, the Committee on Foreign Investment in the United States (CFIUS), the Federal Investment Risk Review Modernization Act of 2018, the Foreign Agent Registration Act (FARA), and others. Furthermore, the electronic systems, although seemingly convenient and efficient, introduce great opportunities for malfeasance because of the complexities and lack of ready transparency they introduce. A return to simple paper ballots that are hand marked and human readable, counted by machines with no printing capability and with traceable receipts confirming that the vote was recorded and maintained in accordance with the intent of the voter is the only way to ensure voting integrity and any audit.

Action 3: All 50 States and Territories must attest in writing to the Secretary of Homeland Security and the Federal Election Commission by Sep 30, 2020 that all electronic and manual aspects of their voting is hosted in the United States of America, and if not, a complete and thorough declaration of what elements of data, processing, and chain of custody are not hosted completely in the United States and a justification of why this hosting and processing does not take place in the United States.

Furthermore, a complete attestation of any transfers of data within or beyond a polling station, the method of transfer (i.e. on line, by hand, by portable media including thumb drives) and an attestation that the transfer of all voting data beyond the county level is conducted over a secure VPN and requiring anyone wishing to upload or access the data for any reason to first register their IP address and a unique identifier. Any failure to completely and legally attest to these matters may warrant the opening of a Department of Justice investigation before the November 2020 election and a declaration that a state or local voting process is invalid. All of this is necessary to assure U.S. Laws such as the Voting Rights Act, RICO, and other Federal and State laws and regulations are being followed. Any State using paper or hard copy votes, which are marked by the voters, and maintained by the State for audit purposes for a period of two years are exempted from the requirements in this action but must attest to their paper or hard copy votes, which are marked by the voters, and maintained by the State for audit purposes for a period of two years.

The entire U.S. election system is vulnerable and likely compromised by illegal access and the actual perpetrators may be veiled in secrecy. It is open to system-wide manipulation. We have observed and gathered compelling evidence of dangerous, substantial interference.



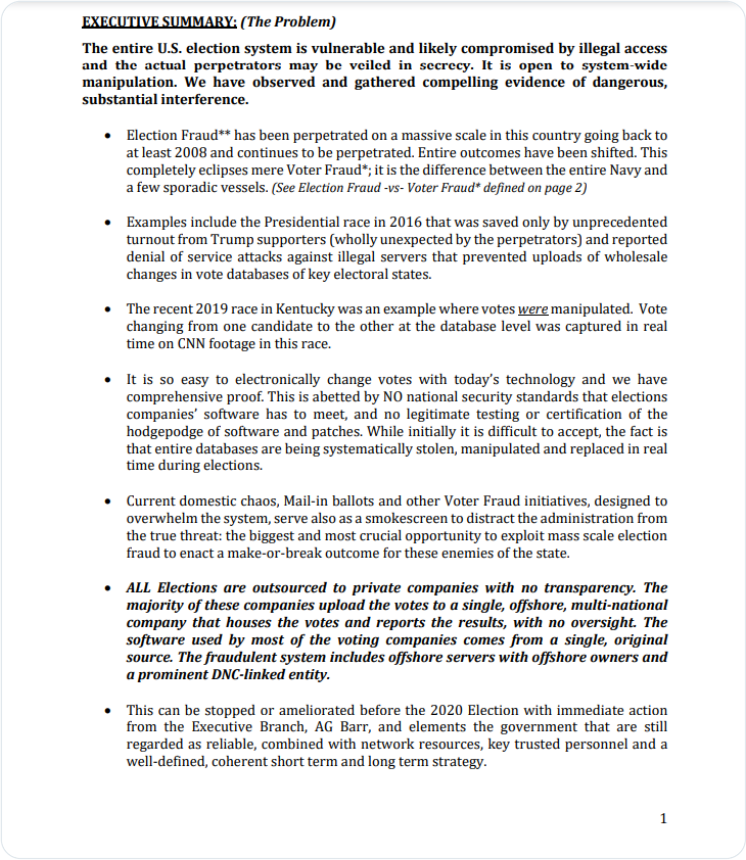
EXECUTIVE SUMMARY: ***(The Problem)***

The entire U.S. election system is vulnerable and likely compromised by illegal access and the actual perpetrators may be veiled in secrecy. It is open to system-wide manipulation. We have observed and gathered compelling evidence of dangerous, substantial interference.

- Election Fraud** has been perpetrated on a massive scale in this country going back to at least 2008 and continues to be perpetrated. Entire outcomes have been shifted. This completely eclipses mere Voter Fraud*; it is the difference between the entire Navy and a few sporadic vessels. *(See Election Fraud -vs- Voter Fraud* defined on page 2)*
- Examples include the Presidential race in 2016 that was saved only by unprecedented turnout from Trump supporters (wholly unexpected by the perpetrators) and reported denial of service attacks against illegal servers that prevented uploads of wholesale changes in vote databases of key electoral states.
- The recent 2019 race in Kentucky was an example where votes *were* manipulated. Vote changing from one candidate to the other at the database level was captured in real time on CNN footage in this race.
- It is so easy to electronically change votes with today's technology and we have comprehensive proof. This is abetted by NO national security standards that elections companies' software has to meet, and no legitimate testing or certification of the hodgepodge of software and patches. While initially it is difficult to accept, the fact is that entire databases are being systematically stolen, manipulated and replaced in real time during elections.
- Current domestic chaos, Mail-in ballots and other Voter Fraud initiatives, designed to overwhelm the system, serve also as a smokescreen to distract the administration from the true threat: the biggest and most crucial opportunity to exploit mass scale election fraud to enact a make-or-break outcome for these enemies of the state.
- ***ALL Elections are outsourced to private companies with no transparency. The majority of these companies upload the votes to a single, offshore, multi-national company that houses the votes and reports the results, with no oversight. The software used by most of the voting companies comes from a single, original source. The fraudulent system includes offshore servers with offshore owners and a prominent DNC-linked entity.***
- This can be stopped or ameliorated before the 2020 Election with immediate action from the Executive Branch, AG Barr, and elements the government that are still regarded as reliable, combined with network resources, key trusted personnel and a well-defined, coherent short term and long term strategy.

1

Election Fraud** has been perpetrated on a massive scale in this country going back to at least 2008 and continues to be perpetrated. Entire outcomes have been shifted. This completely eclipses mere Voter Fraud.



EXECUTIVE SUMMARY: ***(The Problem)***

The entire U.S. election system is vulnerable and likely compromised by illegal access and the actual perpetrators may be veiled in secrecy. It is open to system-wide manipulation. We have observed and gathered compelling evidence of dangerous, substantial interference.

- Election Fraud** has been perpetrated on a massive scale in this country going back to at least 2008 and continues to be perpetrated. Entire outcomes have been shifted. This completely eclipses mere Voter Fraud*; it is the difference between the entire Navy and a few sporadic vessels. *(See Election Fraud -vs- Voter Fraud* defined on page 2)*
- Examples include the Presidential race in 2016 that was saved only by unprecedented turnout from Trump supporters (wholly unexpected by the perpetrators) and reported denial of service attacks against illegal servers that prevented uploads of wholesale changes in vote databases of key electoral states.
- The recent 2019 race in Kentucky was an example where votes *were* manipulated. Vote changing from one candidate to the other at the database level was captured in real time on CNN footage in this race.
- It is so easy to electronically change votes with today's technology and we have comprehensive proof. This is abetted by NO national security standards that elections companies' software has to meet, and no legitimate testing or certification of the hodgepodge of software and patches. While initially it is difficult to accept, the fact is that entire databases are being systematically stolen, manipulated and replaced in real time during elections.
- Current domestic chaos, Mail-in ballots and other Voter Fraud initiatives, designed to overwhelm the system, serve also as a smokescreen to distract the administration from the true threat: the biggest and most crucial opportunity to exploit mass scale election fraud to enact a make-or-break outcome for these enemies of the state.
- ***ALL Elections are outsourced to private companies with no transparency. The majority of these companies upload the votes to a single, offshore, multi-national company that houses the votes and reports the results, with no oversight. The software used by most of the voting companies comes from a single, original source. The fraudulent system includes offshore servers with offshore owners and a prominent DNC-linked entity.***
- This can be stopped or ameliorated before the 2020 Election with immediate action from the Executive Branch, AG Barr, and elements the government that are still regarded as reliable, combined with network resources, key trusted personnel and a well-defined, coherent short term and long term strategy.

1

2016 Presidential race was saved only by unprecedented turnout from Trump supporters (wholly unexpected by the perpetrators) and reported denial of service attacks against illegal servers that prevented uploads of wholesale changes in vote databases of key electoral states

EXECUTIVE SUMMARY: ***(The Problem)***

The entire U.S. election system is vulnerable and likely compromised by illegal access and the actual perpetrators may be veiled in secrecy. It is open to system-wide manipulation. We have observed and gathered compelling evidence of dangerous, substantial interference.

- Election Fraud** has been perpetrated on a massive scale in this country going back to at least 2008 and continues to be perpetrated. Entire outcomes have been shifted. This completely eclipses mere Voter Fraud*; it is the difference between the entire Navy and a few sporadic vessels. *(See Election Fraud -vs- Voter Fraud* defined on page 2)*
- Examples include the Presidential race in 2016 that was saved only by unprecedented turnout from Trump supporters (wholly unexpected by the perpetrators) and reported denial of service attacks against illegal servers that prevented uploads of wholesale changes in vote databases of key electoral states.
- The recent 2019 race in Kentucky was an example where votes *were* manipulated. Vote changing from one candidate to the other at the database level was captured in real time on CNN footage in this race.
- It is so easy to electronically change votes with today's technology and we have comprehensive proof. This is abetted by NO national security standards that elections companies' software has to meet, and no legitimate testing or certification of the hodgepodge of software and patches. While initially it is difficult to accept, the fact is that entire databases are being systematically stolen, manipulated and replaced in real time during elections.
- Current domestic chaos, Mail-in ballots and other Voter Fraud initiatives, designed to overwhelm the system, serve also as a smokescreen to distract the administration from the true threat: the biggest and most crucial opportunity to exploit mass scale election fraud to enact a make-or-break outcome for these enemies of the state.
- ***ALL Elections are outsourced to private companies with no transparency. The majority of these companies upload the votes to a single, offshore, multi-national company that houses the votes and reports the results, with no oversight. The software used by most of the voting companies comes from a single, original source. The fraudulent system includes offshore servers with offshore owners and a prominent DNC-linked entity.***
- This can be stopped or ameliorated before the 2020 Election with immediate action from the Executive Branch, AG Barr, and elements the government that are still regarded as reliable, combined with network resources, key trusted personnel and a well-defined, coherent short term and long term strategy.

1

Now let's review some links discussed inside this report. Read further up in my thread and you will see Scytl aka Clarity Elections and how they have grown in the US.

Well they have a vulnerability that provides the ability to alter votes undetected.

⚔️😈🌹Bad Kitty 真相🌹😈⚔️
@pepesgrandma

Replying to @pepesgrandma

2019 - Switzerland Researchers have found a severe issue in the Barcelona headquartered Scytl aka Clarity Elections voting system that they say would let someone alter votes undetected. They halted use of this in Switzerland. This operates in the US.

Researchers Find Critical Backdoor in Swiss Online Voting System
Researchers have found a severe issue in the new Swiss internet voting system that they say would let someone alter votes undetected. They …
🔗 vice.com

7:46 AM · Nov 7, 2020

101 84 people are Tweeting about this

Read all about the investors in Scytl aka Clarity Elections in this article. And find that interwoven into its very core is the CIAs IN-Q-TEL.

This article was discussed in the document. Imagine the CIA with a voting vulnerability in their hands.😱

⚔️😈🌹Bad Kitty 真相🌹😈⚔️
@pepesgrandma

How Investors Re-appropriate Intelligence Tools to Change Your Vote.

Welcome to the world of Scytl, a Spanish-based co that counts some US, US overseas, and European military votes. It has the technology to manufacture, manipulate and rig vote counts.

How the intelligence community controls your vote
Critics of internet and computer voting have an axiom: the election is never over until the cybervote comes in. Now there is a Spanish-based …
freepress.org

8:16 AM · Nov 7, 2020

183 189 people are Tweeting about this

• • •